**IT Applications, Ch 7, Information Management**

Threats to the integrity and security of data and information stored, communicated and disposed of by organisations.

Complete the following from p 270-

**Deliberate threats**

1. When does intentional damage occur?

Intentional damage occurs when a group or individual deliberately sets out to cause problems within an information system. Their aim may be to cause damage to the hardware or alter the data in some way.

1. Unauthorised access is both physical and logical. Explain what this means?
2. Computer Virus
   1. Describe the nature of this virus.

A computer virus infects a machine in much the same manner a biological virus infects a human; there are also many types of computer viruses.

* 1. What is the main purpose of a virus?

The main purpose of a computer virus is to affect the running of a computer in a way unintended by the user.

* 1. What is meant by the term, payload?

The term payload refers to the action that the virus is designed to carry out, such as deleting files from the hard disk or randomly sending email to recipients found in the address book.

* 1. Describe a worm?

A worm is a virus which replicates itself to take up space on the hard disk on a single workstation.

* 1. List the other types of viruses, p 272, fig. 7-10.

Other types of viruses include:

* Boot infections: attacks the critical section of the hard drive, therefore when the computer boots up, the malicious code is launched by the system and the computer is vulnerable to intruders.
* Executable: an executable is a file that has been affected by a virus. Therefore the virus is run before the file is loaded and may modify it in some way.
* Macro: a macro is common on computers running Microsoft Office applications, and is executed when the infected file is loaded.
* Time bomb: a time bomb refers to an action which is triggered to occur at certain date and time.
* Logic bomb: refers to an action based on a certain condition being met.
* Trojan horse: this refers to a virus hidden within a normal application, which when run starts to infect the system.
* Resident: a resident virus functions by installing malicious code into the memory of the computer, infecting programs currently installed on the hard drive and other future programs.
* Polymorphic: polymorphic viruses encrypt themselves in a different way each time they infect a system. This type of virus is very hard for antivirus programs to detect as it tends to duplicate itself in large numbers.
  1. How do viruses mainly spread?

Viruses mainly spread through an email file attachment or by the transfer of the infected files on removable storage devices.

1. Hacking/Cracking
   1. Who is a hacker and what damage do they cause?

A hacker is a person who gains unauthorised access to an information system through logical means in order to look at the stored data or simply for the challenge. A hacker may use the information they gain blackmail an organisation or highlight security holes in a network.

1. Tampering with files
   1. Describe how employees tamper with files.

Employees can tamper with files by adjusting salary amounts, erasing important medical documents (about patient’s details from hospital databases), or even changing research findings (to suit certain stakeholders).

* 1. What is industrial sabotage?

Industrial sabotage refers to ruining something

1. Information theft
   1. Why does this occur?

Information theft occurs because all organisations look for an edge over their competitors; this can lead to less scrupulous businesses resorting to the theft of information of other competitors.

1. Vandalism of hardware

Vandalism of hardware refers to the deliberate damage of equipment, for example every week in Victoria alone vandals will deliberately damage automatic ticket machines.

1. Theft of hardware

The theft of hardware occurs because computer hardware is often in great demand. Large desktop computers are too bulky and not cost-effective to steal but smaller items that are easier to conceal and bring a better ‘return’ are more likely to be stolen.

**Accidental threats**

1. User error
   1. List some common examples of user error.

Common examples of user error are:

* Copying an older version of the file over a newer version
* Formatting a disk that contains important data
* Not shutting hardware down properly (potentially leading to corrupted files or damaged components)
  1. What processes are in place to limit user error?

Many programs try to limit the amount data lost by users by asking them to confirm certain actions. For example most programs will ask a user if they wish to save changes to a document before closing it and will request confirmation before sending a document.

1. Failure to follow file-management procedures
   1. List common errors of employees in saving files.

Common errors of employees in saving files are:

* File extensions being left off
* Non-descriptive file names have been used
* Folders have been used improperly

**Technical Failure**

1. List some examples of technical failure.

Technical failures can include:

* The failure of a computers CPU
* The failure of a computers CD drive
* The failure of a computers graphic card
* The failure of a computer’s hard disk

**Consequences of violating security and privacy measures, p 278**

1. List three important consequences if security measures are violated.

If security measures are violated the consequences can be:

* Breaches of privacy
* Loss of intellectual property
* Loss of income due to unavailability of information or services

Darcie Anderson